ON SKEW POLYNOMIAL CODES AND LATTICES FROM QUOTIENTS OF CYCLIC DIVISION ALGEBRAS

JÉRÔME DUCOAT AND FRÉDÉRIQUE OGGIER

Abstract. We propose a variation of Construction A of lattices from linear codes defined using the quotient $\Lambda/\mathfrak{p}\Lambda$ of some order Λ inside a cyclic division F-algebra, for $\mathfrak{p}$ a prime ideal of a number field F. To obtain codes over this quotient, we first give an isomorphism between $\Lambda/\mathfrak{p}\Lambda$ and a ring of skew polynomials. We then discuss definitions and basic properties of skew polynomial codes, which are needed for Construction A, but also explore further properties of the dual of such codes. We conclude by providing an application to space-time coding, which is the original motivation to consider cyclic division F-algebras as a starting point for this variation of Construction A.

1. Introduction

Connections between Euclidean lattices and linear codes over finite alphabets have been classically studied, through a series of constructions referred to as Constructions A,B,C,D or E [1]. Given the finite field $\mathbb{F}_2$, the original (binary) Construction A [2] considers the map $\rho : \mathbb{Z}^N \to \mathbb{F}_2^N$ of reduction modulo 2 componentwise, for N some positive integer. If C is a binary linear code of length N, then $\rho^{-1}(C)$ (or its normalized version $\frac{1}{\sqrt{2}}\rho^{-1}(C)$) is a lattice. A series of duality follows, such as a correspondence between the dual code $C^{\perp}$ of C and the dual lattice L^* of L, self-dual codes and unimodular lattices, or between the weight enumerator of the code C and the theta series of the lattice L. Construction A has been generalized in many ways, including, for citing a few examples, to: (1) cyclotomic fields $\mathbb{Q}(\zeta_p)$ [3], where ζ_p is a primitive pth root of unity, and p is prime, in which case ρ becomes the componentwise reduction modulo the prime ideal $(1-\zeta_p)$ of a vector with coefficients in the ring of integers $\mathbb{Z}[\zeta_p]$, (2) to quadratic and imaginary fields and totally definite quaternion algebras over $\mathbb{Q}$ as a way to construct modular lattices in [4], (3) to the construction of unimodular lattices using quaternary quadratic residue codes [5].

Construction A is also of interest from a communication point of view, since it provides a concrete way of doing coset coding [2], an encoding technique which is very useful to encode lattices, since it provides a natural way of mapping elements from finite alphabets (codewords) to real or complex symbols (lattice points).

This paper addresses a variation of Construction A in the context of division algebras, and cyclic division algebras over a cyclic number field extension K/F in particular. Denote by $\mathcal{O}_F$ and $\mathcal{O}_K$ their respective rings of integers, and by σ the

1991 *Mathematics Subject Classification.* Primary 11S45; Secondary 11T71, 94B40.

Key words and phrases. Constacyclic codes, Division algebras, Skew polynomial rings, Space-time codes.

The research of J. Ducoat and F. Oggier was supported by the Singapore National Research Foundation under Research Grant NRF-RF2009-07.

generator of the Galois group of K/F. Instead of using as a starting point the quotient of a number field by an ideal (as in [3] for example), we consider a specific $\mathcal{O}_F$-order Λ in a cyclic division F-algebra, and the quotient $\Lambda/\mathfrak{p}\Lambda$ for $\mathfrak{p}$ a prime ideal of $\mathcal{O}_F$.

As shown in Section 2, the quotient $\Lambda/\mathfrak{p}\Lambda$ turns out to be isomorphic to the ring of skew polynomials $(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[x;\sigma]/(x^n-u)$, where u is determined by the choice of the cyclic division F-algebra. To mimic the steps involved in Construction A, we next consider the problem of designing codes over $(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[x;\sigma]/(x^n-u)$ in Section 3, where a variation of Construction A is given. Let $\mathbb{F}_q$ denote the finite field with q elements, q a prime power. Codes over the skew polynomial ring $\mathbb{F}_q[x;\sigma]/(f(x))$, for $(f(x))$ a two sided ideal of $\mathbb{F}_q[x;\sigma]$, were introduced in [6] and furthermore studied in the context of cyclic codes in [7]. A generalization to Galois rings was obtained in [8]. We propose some basic definitions and properties of codes over the skew polynomial ring $(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[x;\sigma]/(x^n-u)$, by taking inspiration from [8] and generalizing some of the known results for the ring $\mathbb{F}_q[x;\sigma]/(x^n-u)$. We note that our results could be easily generalized to the case $(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[x;\sigma]/(f(x))$, which is not done in this paper because of our focus on cyclic division algebras.

Once equipped with suitable definitions for skew polynomial codes over the ring $(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[x;\sigma]/(x^n-u)$, it is natural to wonder about the dual of such codes. This is studied in Section 4.

We conclude by going back to the original motivation to consider this variation of Construction A over a cyclic division F-algebra, namely its application to space-time coding, or more precisely, to derive a way to perform coset encoding, as detailed in Section 5.

2. Quotients of Cyclic Division Algebras

Let K/F be a number field extension of degree n with cyclic Galois group $\langle\sigma\rangle$, and respective rings of integers $\mathcal{O}_K$ and $\mathcal{O}_F$. Consider the cyclic F-algebra A defined by

$$K \oplus Ke \oplus \cdots Ke^{n-1}$$

where $e^n = u \in F$, and $ek = \sigma(k)e$ for $k \in K$. We assume that u^i, $i = 0, \dots, n-1$, are not norms in K/F so that the algebra is division.

For S a Noetherian integral domain with quotient field F, and A a finite dimensional F-algebra, an S-order in A is a subring Λ of A, having the same identity as A, and such that Λ is a finitely generated module over S and generates A as a linear space over F. An order Λ is called maximal if it is not properly contained in any other S-order.

Then

$$\Lambda = \mathcal{O}_K \oplus \mathcal{O}_K e \oplus \cdots \oplus \mathcal{O}_K e^{n-1}$$

is an $\mathcal{O}_F$-order of A, which is typically not maximal.

Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_F$ so that $\mathfrak{p}\Lambda$ is a two-sided ideal of Λ, and $\mathcal{O}_F/\mathfrak{p}\mathcal{O}_F$ is the finite field $\mathbb{F}_{p^f}$, where p is the prime number lying below $\mathfrak{p}$ and f is the inertial degree of $\mathfrak{p}$ above p. Since Λ is an $\mathcal{O}_F$-module, we have the following ring homomorphism :

$$\mathcal{O}_F \to \Lambda \to \Lambda/\mathfrak{p}\Lambda$$

and the image of $\mathfrak{p} = \mathfrak{p}\Lambda \cap \mathcal{O}_F$ obviously lies in $\mathfrak{p}\Lambda$. Hence, it yields a ring homomorphism $\mathbb{F}_{p^f} = \mathcal{O}_F/\mathfrak{p} \to \Lambda/\mathfrak{p}\Lambda$, which means that $\Lambda/\mathfrak{p}\Lambda$ is an $\mathbb{F}_{p^f}$-algebra.

From [9], we have the following $\mathbb{F}_{p^f}$-algebra isomorphism :

$$\Lambda/\mathfrak{p}\Lambda \simeq (\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K) \oplus (\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)e \oplus \cdots \oplus (\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)e^{n-1},$$

where $e(k + \mathfrak{p}\mathcal{O}_K) = (\sigma(k) + \mathfrak{p}\mathcal{O}_K)e$ for all $k \in \mathcal{O}_K$ and $e^n = u + \mathfrak{p}$.

Indeed, since $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_F$ and $\sigma_{|F} = \mathrm{Id}_F$, we have $\sigma(\mathfrak{p}\mathcal{O}_K) \subset \mathfrak{p}\mathcal{O}_K$, which means that σ can be factorized as a ring homomorphism by the natural projection $\pi : \mathcal{O}_K \to \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$: more explicitely, there exists a ring homomorphism $\overline{\sigma} : \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K \to \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$ such that $\sigma = \overline{\sigma} \circ \pi$. By a slight abuse of notation, we keep the notation σ for the map $\overline{\sigma}$.

Since $\mathcal{O}_K$ is a Dedekind domain, $\mathfrak{p}\mathcal{O}_K = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_g^{e_g}$ with $\mathfrak{p}_i$ a prime ideal of $\mathcal{O}_K$ and $e_i \geq 0$ for $i = 1, \ldots, g$.

In the particular case where $\mathfrak{p}$ is inert in K/F, $\mathfrak{p}\mathcal{O}_K$ is a prime ideal of $\mathcal{O}_K$. Then the finite ring $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$ is an integral domain, so it is the finite field $\mathbb{F}_{p^{nf}}$. The induced ring homomorphism $\sigma : \mathbb{F}_{p^{nf}} = \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K \to \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K = \mathbb{F}_{p^{nf}}$ is thus a generator of the cyclic Galois group of $\mathbb{F}_{p^{nf}}/\mathbb{F}_{p^f}$.

Given a ring S with a group $G = \langle\sigma\rangle$ acting on it, the skew polynomial ring $S[x;\sigma]$ is the set of all polynomials $s_0 + s_1x + \ldots + s_mx^m$, $s_i \in S$, $m \geq 0$ with multiplication twisted by the relation $xs = \sigma(s)x$ for all $s \in S$.

We will consider the skew polynomial ring $(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[x;\sigma]$. Note that since $u \in F$, $x^n - u$ belongs to the center of $(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[x;\sigma]$ and the ideal $(x^n - u)$ is two-sided.

Lemma 2.1. *There is an $\mathbb{F}_{p^f}$-algebra isomorphism between $\Lambda/\mathfrak{p}\Lambda$ and the quotient of $(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[x;\sigma]$ by the two-sided ideal generated by $x^n - u$.*

Proof. We define the map

$$\begin{aligned}\varphi : (\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[x;\sigma] &\to \Lambda/\mathfrak{p}\Lambda\\ f(x) &\mapsto f(e).\end{aligned}$$

Using the isomorphism given above and in [9], it is easily seen that φ is a surjective $\mathbb{F}_{p^f}$-algebra homomorphism. Moreover, the kernel of φ is the two-sided ideal of $(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[x;\sigma]$ generated by $x^n - u$. Indeed, it is easily seen that $x^n - u$ lies in $\ker(\varphi)$. Conversely, let $f(x) \in \ker(\varphi)$. We write

$$f(x) = \sum_{i=0}^{m} s_ix^i,\ s_i \in \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K,\ i = 0, ..., m.$$

Then $f(e) = 0$ in $\Lambda/\mathfrak{p}\Lambda$. The ring $(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[x;\sigma]$ is not always right or left Euclidean, as it would be if $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$ were a finite field. However, since $x^n - u$ is a monic polynomial (or more precisely since its leading coefficient is a unit in $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$), we can still perform the long division algorithm: indeed, if $m \geq n$, we may perform a right division of $f(x)$ by $x^n - u$ as follows. Note that the polynomial

$$f(x) - s_mx^{m-n}(x^n - u) = \sum_{i=0}^{m-1} s_ix^i + s_mux^{m-n}$$

has degree smaller than that of f. This procedure of subtracting left multiple of $x^n - u$ can be repeated until we obtain a polynomial of degree smaller than n, thus, there exist some polynomials $g(x)$ and $h(x)$ such that

$$f(x) = g(x)(x^n - u) + h(x)$$

where $h(x)$ has degree $\leq n - 1$. Hence, $f(e) = 0$ is equivalent to $h(e) = 0$. Yet, $0 = h(e) = r_0 + r_1e + \cdots + r_{n-1}e^{n-1}$ in $\Lambda/\mathfrak{p}\Lambda \simeq (\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K) \oplus (\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)e \oplus \cdots \oplus$

$(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)e^{n-1}$. Therefore, $r_0 = r_1 = \cdots = r_{n-1} = 0$ and $h(x) = 0$. We conclude that $f(x)$ is a (left) multiple of $x^n - u$. Consequently, $\ker(\varphi) = (x^n - u)$ and we get the desired isomorphism. □

This lemma generalizes the isomorphism of [10, Lemma 1] for $\mathfrak{p}$ inert.

Denote by ψ the inverse isomorphism of the one given in Lemma 2.1:

$$\psi : \Lambda/\mathfrak{p}\Lambda \cong (\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[x;\sigma]/(x^n - u).$$

Let $\mathcal{I}$ be a left ideal of Λ. Assume that $\mathcal{I} \cap \mathcal{O}_F \supset \mathfrak{p}$. Then $\mathcal{I}/\mathfrak{p}\Lambda$ is an ideal of $\Lambda/\mathfrak{p}\Lambda$. In the sequel, we will study the left ideal $\psi(\mathcal{I}/\mathfrak{p}\Lambda)$ of $(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[x;\sigma]/(x^n - u)$.

3. Skew-Polynomial Codes and a Variation of Construction A

Classical cyclic codes over the finite field $\mathbb{F}_q$ are ideals of the polynomial ring $\mathbb{F}_q[x]/(x^n - 1)$. Since this is a principal ideal domain, every ideal has a generator polynomial, which in turn defines a cyclic code, and codewords are then multiples of this generator polynomial. In [6], the definition of codes over polynomial rings was extended to that of codes over the skew-polynomial rings $\mathbb{F}_q[x;\sigma]$. We are interested here in codes over the skew-polynomial rings $(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[x;\sigma]/(x^n - u)$.

3.1. **Division in Skew-Polynomial Rings.** A first major difference between $\mathbb{F}_q[x;\sigma]$ and $(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[x;\sigma]$ is, as noted in the proof of Lemma 2.1, that the skew polynomial ring $(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[x;\sigma]$ is not in general right or left Euclidean anymore. However, this can be sorted out, using the same technique as that explained in [8], which was also used for the proof of Lemma 2.1.

Let $f(x) = \sum_{i=0}^{m} s_i x^i$ and $g(x) = \sum_{i=0}^{l} t_i x^i$ be two polynomials of respective degree m and l, with coefficients in $(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)$. Suppose that t_l is invertible and $m > l$, then a right (respectively left) division of $f(x)$ by $g(x)$ is obtained as follows: consider the polynomial

$$f(x) - \frac{s_m}{\sigma^{m-l}(t_l)} x^{m-l} g(x)$$

respectively

$$f(x) - g(x)\sigma^{-l}\left(\frac{s_m}{t_l}\right) x^{m-l}.$$

Since σ is an automorphism, $1 = \sigma(t_l t_l^{-1}) = \sigma(t_l)\sigma(t_l^{-1})$, which implies that $\sigma(t_l)$ is invertible. Hence, $\sigma^j(t_l)$ also is invertible for all $1 \leq j \leq m$. Moreover, we have

$$\begin{aligned} f(x) - \frac{s_m}{\sigma^{m-l}(t_l)} x^{m-l} g(x) &= f(x) - s_m x \sigma^{m-l-1}(t_l^{-1}) x^{m-l} g(x) = \cdots \\ &= f(x) - s_m x^{m-l} \sigma^{m-l-(m-l)}(t_l^{-1}) g(x) \\ &= f(x) - s_m x^{m-l} t_l^{-1}(t_l x^l + \sum_{i=0}^{l-1} t_i x^i) \\ &= f(x) - s_m x^m + \sum_{i=0}^{l-1} s_m t_l^{-1} t_i x^i. \end{aligned}$$

Similarly, we have

$$\begin{aligned}
f(x) - g(x)\sigma^{-l}\left(\frac{s_m}{t_l}\right)x^{m-l} &= f(x) - \sum_{i=0}^{l} t_i x^i \sigma^{-l}\left(\frac{s_m}{t_l}\right)x^{m-l} \\
&= f(x) - \sum_{i=1}^{l} t_i x^{i-1}\sigma^{1-l}\left(\frac{s_m}{t_l}\right)x^{m-l+1} - t_0\sigma^{-l}\left(\frac{s_m}{t_l}\right)x^{m-l} \\
&= \cdots \\
&= f(x) - \sum_{i=0}^{l} t_i \sigma^{i-l}\left(\frac{s_m}{t_l}\right)x^{m-l+i} \\
&= f(x) - s_m x^m - \sum_{i=0}^{l-1} t_i \sigma^{i-l}\left(\frac{s_m}{t_l}\right)x^{m-l+i}.
\end{aligned}$$

Hence, both polynomials $f(x) - \frac{s_m}{\sigma^{m-l}(t_l)}x^{m-l}g(x)$ and $f(x) - g(x)\sigma^{-l}\left(\frac{s_m}{t_l}\right)x^{m-l}$ have degree $< m$. Therefore this procedure can be iterated, to find polynomials $q(x), r(x)$ such that

$$f(x) = q(x)g(x) + r(x), \text{ resp. } f(x) = g(x)q(x) + r(x), \ \deg(r(x)) < \deg(g(x)).$$

If $r(x) = 0$, we say that $g(x)$ is a right, resp. left, divisor of $f(x)$.

We next discuss the unicity of the remainder of this division. Suppose

$$f(x) = q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x)$$

then $(q_1(x) - q_2(x))g(x) = r_2(x) - r_1(x)$. Suppose that $q_1(x) - q_2(x)$ is not zero, then the degree of $(q_1(x) - q_2(x))g(x)$ is greater than $\deg(g(x))$, while the degree of $r_2(x) - r_1(x)$ is less than $\deg(g(x))$, therefore $q_1(x) = q_2(x)$ and $r_1(x) = r_2(x)$. The proof for left division is done similarly.

3.2. **Principal Ideals and Codes.**

Thanks to the unicity of the remainder, the skew polynomials of degree less than n are canonical representatives of the elements of $(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[x;\sigma]/(x^n - u)$.

Lemma 3.1. *Any right divisor $g(x)$ of $x^n - u$ generates a left principal ideal $(g(x))/(x^n - u)$ of $(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[x;\sigma]/(x^n - u)$. The set of left multiples of $g(x)$ by skew polynomials of degree $k = n - \deg(g(x))$ are canonical representatives of the elements of $(g(x))/(x^n - u)$.*

Proof. For any right divisor $g(x)$ of $x^n - u$, the ideal $(x^n - u)$ is contained in $(g(x))$. By the correspondence theorem for rings, $(g(x))/(x^n - u)$ is a left ideal of $(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[x;\sigma]/(x^n - u)$. Since skew polynomials of degree less than n are canonical representatives, the elements of the ideal $(g(x))/(x^n - u)$ are left multiples of $g(x)$ by skew polynomials of degree less than $k = n - \deg g(x)$. □

Corollary 1. *For $g(x)$ a right divisor of $x^n - u$, the ideal $(g(x))/(x^n - u)$ is an $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$-module, isomorphic to a submodule of $(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)^n$. It forms a code of length n and of dimension $k = n - \deg g(x)$ over $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$, consisting of codewords $a = (a_0, a_1, \ldots, a_{n-1})$ that are coefficient tuples of the left multiples $a(x) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1}$ of $g(x)$. This code is called a σ-*constacyclic code*.*

Proof. Let $g(x)$ be a right divisor of $x^n - u$ in $(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[x;\sigma]$. The left ideal $(g(x))$ in $(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[x;\sigma]$ is then an $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$-module and by taking the quotient by the monic skew-polynomial $x^n - u$, $(g(x))/(x^n - u)$ is a submodule of the free $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$-module $(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[x;\sigma]/(x^n-u)$ of rank n. By Lemma 1, the images of the skew polynomials $g(x), xg(x), ..., x^{k-1}g(x)$ in the quotient ring $(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[x;\sigma]/(x^n-u)$ form a basis of $g(x)/(x^n-u)$ as an $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$-module. We then use the $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$-module isomorphism

$$\begin{aligned}(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[x;\sigma]/(x^n-u) \quad &\to (\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)^n \\ \sum_{i=0}^{n-1} a_i x^i + (x^n-u)(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[x;\sigma] &\mapsto (a_0, ..., a_{n-1})\end{aligned}$$

to conclude. □

Note that for a σ-constacyclic code $\mathcal{C}$, corresponding to a left principal ideal $\mathcal{I}$ of $(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[x;\sigma]/(x^n-u)$, if $(a_0, \ldots, a_{n-1}) \in \mathcal{C}$, then $a(x) = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1} \in \mathcal{I}$, and $xa(x) \in \mathcal{I}$. Since

$$xa(x) = x(a_0 + a_1 x + \ldots + a_{n-1}x^{n-1}) = \sigma(a_0)x + \sigma(a_1)x^2 + \ldots + \sigma(a_{n-1})u$$

we have that

$$(u\sigma(a_{n-1}), \sigma(a_0), \ldots, \sigma(a_{n-1})) \in \mathcal{C},$$

which explains the choice of the terminology "constacyclic".

Let us comment on the proposed definition of σ-constacyclic code.

(1) We could also use the terminology *central σ-code* proposed in [6] since $x^n - u$ lies in the center of $(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[x;\sigma]$.
(2) A cyclic code would correspond to the case $u = 1$.
(3) This definition could be made more general by considering another suitable polynomial than $x^n - u$, which would yield a complete generalization of the definition of *σ-code* proposed in [6]. This is not done here, simply because the polynomial is given by the cyclic algebra structure, but this could be an interesting research direction of its own.
(4) Finally, we may (and do) restrict our study of σ-constacyclic codes to right divisors $g(x)$ of $x^n - u$ that are monic : indeed, if $g(x)$ has leading coefficient a, it is necessarily invertible (since $g(x)$ is a divisor of $x^n - u$) and the constacyclic codes derived from $g(x)$ and $a^{-1}g(x)$ are equal.

The next result describes a parity check polynomial.

Proposition 1. *Set $h(x) = \sum_{i=0}^{k-1} h_i x^i + x^k$. If $h(x)g(x) = x^n - u$, then*

$$g(x)h(x) = x^n - u.$$

Furthermore, let $\mathcal{C}$ be the code generated by $g(x)$. Let $a \in (\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)^n$ and let $a(x)$ be its corresponding polynomial. Then a is a codeword of $\mathcal{C}$ if and only if $a(x)h(x) = 0$ in $(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[x;\sigma]/(x^n-u)$.

Proof. Since $x^n - u$ is central,

$$h(x)g(x)h(x) = (x^n-u)h(x) = h(x)(x^n-u) = h(x)h(x)g(x)$$

and

$$h(x)[g(x)h(x) - h(x)g(x)] = 0.$$

The first claim follows from the fact that $h(x)$ is monic and thus not a zero divisor.

If $a \in \mathcal{C}$ then $a(x) = b(x)g(x)$ and using the first claim

$$a(x)h(x) = b(x)g(x)h(x) = 0 \mod x^n - u.$$

Conversely, if $a(x)h(x) = 0$, then for some $b(x)$, $a(x)h(x) = b(x)(x^n - u) = b(x)g(x)h(x)$. Since $h(x)$ is monic and thus not a zero divisor, $a(x) = b(x)g(x)$ as needed. □

3.3. **A Construction A.** Using the isomorphism ψ defined in Section 2, for every left ideal $\mathcal{I}$ of Λ, we consider the σ-code $\mathcal{C} = \psi(\mathcal{I}/\mathfrak{p}\Lambda)$ over $\mathbb{F}_q$.

A lattice of dimension N is here a discrete additive subgroup of $\mathbb{R}^N$ of rank N as a $\mathbb{Z}$-module.

We set the map :

$$\rho : \Lambda \to \psi(\Lambda/\mathfrak{p}\Lambda) = \mathbb{F}_q[x;\sigma]/(x^n - u),$$

compositum of the canonical projection $\Lambda \to \Lambda/\mathfrak{p}\Lambda$ with ψ. Then

$$L = \rho^{-1}(\mathcal{C}) = \mathcal{I}$$

is a lattice in $\mathbb{R}^N$, that is a $\mathbb{Z}$-module of rank $N = n^2[F : \mathbb{Q}]$ since $\mathcal{O}_K$ is a $\mathbb{Z}$-module of rank $n[F : \mathbb{Q}]$.

From this point of view, the above construction may be interpreted as a variation of Construction A [1], which consists of obtaining a lattice from a linear code over a finite field (ring), as shortly described in the introduction. This is also a generalization of the lattice construction of [11], defined over number fields.

3.4. **Examples.** Let $K = \mathbb{Q}(i)$ and $F = \mathbb{Q}$. Then $\mathcal{O}_F = \mathbb{Z}$ and $\mathcal{O}_K = \mathbb{Z}[i]$. Let $\mathfrak{Q}$ be the quaternion division algebra defined by

$$\mathfrak{Q} = \mathbb{Q}(i) \oplus \mathbb{Q}(i)e,$$

with $e^2 = -1$. Since $N_{K/F}(a + ib) = a^2 + b^2$, $a, b \in \mathbb{Z}$, -1 cannot be a norm and $\mathfrak{Q}$ is indeed a quaternion division algebra. We set $\Lambda = \mathbb{Z}[i] \oplus \mathbb{Z}[i]e$.

We provide different examples based on primes with different ramification.

Example 1. Set $p = 3$, which remains inert in $\mathbb{Q}(i)$. Hence, $\mathbb{Z}[i]/3\mathbb{Z}[i] \simeq \mathbb{F}_9$ and $\Lambda/3\Lambda \simeq \mathbb{F}_9 \oplus \mathbb{F}_9 e$. Take $\mathcal{I} = (1 + i + e)\Lambda$. Then $\mathcal{I}$ contains 3 since the norm of $1 + i + e$ is $N(1 + i + e) = (1 + i + e)(1 - i - e) = 3$. Let α denote a primitive root of $\mathbb{F}_9$ over $\mathbb{F}_3$, satisfying $\alpha^2 + 1 = 0$ and note that σ becomes the generator of the Galois group of $\mathbb{F}_9/\mathbb{F}_3$, $\sigma(\alpha) = \alpha^3$. We have

$$\psi((1 + i + e)\text{mod}3) = 1 + \alpha + x,$$

which is a right divisor of $x^2 + 1$ in $\mathbb{F}_9[x;\sigma]$:

$$(x - 1 + \alpha)(x + 1 + \alpha) = x^2 + \sigma(1 + \alpha)x + (\alpha - 1)x + (\alpha + 1)(\alpha - 1) = x^2 + 1.$$

Therefore, the left ideal $(x + 1 + \alpha)\mathbb{F}_9[x;\sigma]/(x^2 + 1)$ consisting of the left multiples of $x + 1 + \alpha$ modulo $x^2 + 1$ is a σ-constacyclic code of length $n = 2$ and dimension $k = n - \deg g(x) = 1$. Left multiples of $x + 1 + \alpha$ modulo $x^2 + 1$ are explicitly given by $(b_0 + b_1 x)(x + \alpha + 1) = [b_0(\alpha + 1) - b_1] + [b_0 + b_1(1 - \alpha)]x$ and codewords are of the form

$$(a_0, a_1) = ((\alpha + 1)a_1, a_1),\ a_1 \in \mathbb{F}_9.$$

Taking the pre-image by ψ, it corresponds to the left-ideal $\mathcal{I}/3\Lambda$, with $\mathcal{I} = (1 + i + e)\Lambda$.

Example 2. Set $p = 5$, which splits in $\mathbb{Q}(i)$, namely $(5) = (1 + 2i)(1 - 2i)$. Then $\mathbb{Z}[i]/5\mathbb{Z}[i] \simeq \mathbb{Z}[i]/(1+2i)\times\mathbb{Z}[i]/(1-2i) \simeq \mathbb{F}_5\times\mathbb{F}_5$ and $\Lambda \simeq (\mathbb{F}_5\times\mathbb{F}_5)\oplus(\mathbb{F}_5\times\mathbb{F}_5)e$. The first isomorphism comes from the Chinese Remainder Theorem, since $(1 - 2i)$ and $(1+2i)$ are coprime. An element of $\mathbb{Z}[i]$ is mapped to $\mathbb{F}_5 \times \mathbb{F}_5$ via the composition of the natural projection and the above isomorphism by $\pi : a+ib \mapsto (a+2b \mod 5, a+3b \mod 5)$. Since $\pi((a+ib)(c+di)) = \pi(ac-bd+i(ad+bc)) = (ac-bd+2(ad+bc) \mod 5, ac-bd+3(ad+bc) \mod 5)$ while $\pi(a+ib)\pi(c+di) = (a+2b \mod 5, a+3b \mod 5)(c+2d \mod 5, c+3d \mod 5) = (ac+2ad+2cb-bd \mod 5, ac+3ad+3bc-bd \mod 5)$, and $\pi(a+ib+c+id) = a+c+2(b+d) = a+2b+c+2d = \pi(a+ib)+\pi(c+id)$, π is indeed a ring homomorphism. Note that σ becomes $\sigma(a, b) = (b, a)$, which fixes elements of the form (a, a), $a \in \mathbb{F}_5$. Take $\mathcal{I} = (1 + 2e)\Lambda$, which contains 5 since the norm of $\mathcal{I}$ is $N(1 + 2e) = (1 + 2e)(1 - 2e) = 5$. Then

$$\psi((1 + 2e)\mathrm{mod}5) = (1, 1) + (2, 2)x,$$

which is a divisor of $x^2 + 1$, since

$$((1, 1) + (2, 2)x)((1, 1) - (2, 2)x) = (1, 1) - (2, 2)x + (2, 2)x + (1, 1)x^2.$$

Then the left ideal $((1, 1)+(2, 2)x)(\mathbb{F}_5\times\mathbb{F}_5)[x; \sigma]/(x^2+1)$ forms a σ-constacyclic code of length $n = 2$ and $k = 1$. Codewords are of the form $[(b_0, b_1) + (c_0, c_1)x][(1, 1) + (2, 2)x]$ or equivalently, $[(b_0, b_1) + (c_0, c_1)x][(3, 3) + (1, 1)x] = [(3b_0, 3b_1) - (c_0, c_1)] + [(b_0, b_1) + (3c_0, 3c_1)]x$, that is

$$(3a, a),\ a = (a_0, a_1) \in \mathbb{F}_5 \times \mathbb{F}_5.$$

Again, taking the pre-image by ψ, it corresponds to the left-ideal $\mathcal{I}/5\Lambda$, with $\mathcal{I} = (1 + 2e)\Lambda$.

Example 3. Set $p = 2$, which is ramified in $\mathbb{Q}(i)$: $(2) = (1+i)^2$. Then $\mathbb{Z}[i]/2\mathbb{Z}[i] \simeq \mathbb{F}_2+\upsilon\mathbb{F}_2 = \{0, 1, \upsilon, \upsilon+1\}$ with $\upsilon^2 = 0$, and $\Lambda/2\Lambda \simeq (\mathbb{F}_2+\upsilon\mathbb{F}_2)\oplus(\mathbb{F}_2+\upsilon\mathbb{F}_2)e$. In this case, the natural projection π from $\mathbb{Z}[i]$ to $\mathbb{F}_2 + \upsilon\mathbb{F}_2$ is given by $\pi : a + ib \mapsto (a + b) \mod 2+\upsilon(b \mod 2)$. We check that π is a ring homomorphism: $\pi((a+ib)(c+di)) = \pi(ac - bd + i(ad + bc)) = (ac + bd + ad + bc \mod 2) + \upsilon(ad + bc \mod 2)$ while $\pi(a+ib)\pi(c+di) = ((a+b \mod 2)+\upsilon(b \mod 2))((c+d \mod 2)+\upsilon(d \mod 2)) = (a+b)(c+d) \mod 2+(a+b)d\upsilon+b(c+d)\upsilon = (ac+bd+ad+bc)+\upsilon(ad+bc) \mod 2$, as needed, and $\pi(a+ib+c+id) = a+c+b+d+\upsilon(b+d) = a+b+\upsilon b+c+d+\upsilon d = \pi(a + ib) + \pi(c + id)$. Moreover, since $p = 2$ totally ramifies in $\mathbb{Z}[i]$, σ becomes the identity map. Take $\mathcal{I} = (1 + e)\Lambda$, which contains 2 since the norm of $\mathcal{I}$ is $N(1 + e) = (1 + e)(1 - e) = 2$. Then

$$\psi((1 + e)\mathrm{mod}2) = 1 + x,$$

which is a divisor of $x^2 + 1 = (x + 1)(x + 1)$. As in the previous cases, the left ideal $(1 + x)(\mathbb{F}_2 + \upsilon\mathbb{F}_2)[x; \sigma]/(x^2 + 1)$ forms a σ-constacyclic code of length $n = 2$ and $k = 1$. Codewords are of the form $(b_0 + b_1x)(1 + x)$, that is we get the repetition code

$$(a_0, a_1) = (a_0, a_0),\ a_0 \in \mathbb{F}_2 + \upsilon\mathbb{F}_2.$$

As above, taking the pre-image by ψ, it corresponds to the left-ideal $\mathcal{I}/2\Lambda$, with $\mathcal{I} = (1 + e)\Lambda$.

4. Dual Codes and Lattices

Having defined constacyclic codes over $(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[x; \sigma]/(x^n - u)$, it is natural to wonder about the dual of such codes.

4.1. **Dual Codes.** We consider the following Euclidean scalar product in $(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)^n$:

$$\langle y, z\rangle = \sum_{i=1}^{n} y_i z_i.$$

Definition 4.1. For an (n,k) code $\mathcal{C}$, its Euclidean dual code $\mathcal{C}^\perp$ is given by

$$\mathcal{C}^\perp = \{y,\ \langle c, y\rangle = 0 \text{ for all c } \in \mathcal{C}\}.$$

An (n,k) code $\mathcal{C}$ is said to be Euclidean self-dual if $\mathcal{C}$ is equal to its Euclidean dual.

It is probably helpful to recall how the generator polynomial of a cyclic code over a finite field is computed. Take $h(x)$ its parity check polynomial, with degree d and constant term h_0, and compute $h_0^{-1}x^d h(x^{-1})$. The procedure in the case of interest here is somewhat similar, except for one difficulty: we need to give a meaning to $h(x^{-1})$ in the non-commutative case, which is classically done through localization (as also done in [8]). It is known [12, Thm II.2.4] that given a ring R, if $S \subset R$ is a right Ore set, then there is a ring RS^{-1} of right fractions and an injective ring homomorphism $R \to RS^{-1}$ such that (a) the image of every element $r \in R$ is invertible in RS^{-1}, and (b) every element of RS^{-1} can be written as a product rs^{-1}.

Proposition 2. *Consider the ring $(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[x;\sigma]$ as above, and take S to be $S = \{x^i,\ i \geq 0\}$. Then S is a right Ore set, and the right localization $(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[x;\sigma]S^{-1}$ exists. Furthermore, the subring $A = \{\sum_{i=0}^{d} x^{-i}a_i\}$ of $(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[x;\sigma]S^{-1}$, with multiplication $ax^{-1} = x^{-1}\sigma(a)$ is isomorphic to the ring $(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[x^{-1},\sigma^{-1}]$.*

Proof. By definition of Ore set [12, Def. II.2.3], we need to check the following three conditions:

(1) S is closed under multiplication, and $1 \in S$.
(2) For any $s \in S$, s is not a left or right zero divisor.
(3) Right Ore condition: for all $r \in R$ and $s \in S$, there exist $r_1 \in R$ and $s_1 \in S$ such that $sr_1 = rs_1$. Take $s = x^i \in S$ for some i, and $r = r(x) = \sum_{l=0}^{d} r_l x^l \in \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K[x;\sigma]$. We need to show that there exists $r_1 = r_1(x)$ such that $x^i r_1(x) = r(x)x^j$ for some x^j. Pick $j \geq i$ and $r_1(x) = \sum_{l=0}^{d} \sigma^{-i}(r_l)x^{j+l-i}$. Then

$$x^i \sum_{l=0}^{d} \sigma^{-i}(r_l)x^{j+l-i} = \sum_{l=0}^{d} r_l x^{j+l} = r_1(x)x^j$$

as needed to show the existence of the localization $(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[x;\sigma]S^{-1}$.

Next, consider the map

$$\theta : (\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[x;\sigma] \to A,\ \sum_{i=0}^{d} a_i x^i \mapsto \sum_{i=0}^{d} x^{-i}a_i.$$

We have, assuming without loss of generality that $t \geq d$ and $a_{d+1} = \ldots = a_t = 0$, that

$$\theta(\sum_{i=0}^{d} a_i x^i + \sum_{i=0}^{t} b_i x^i) = \theta(\sum_{i=0}^{t}(a_i + b_i)x^i) = \theta(\sum_{i=0}^{d} a_i x^i) + \theta(\sum_{i=0}^{t} b_i x^i)$$

and

$$\begin{aligned}\theta(\sum_{i=0}^{d} a_i x^i \sum_{i=0}^{t} b_i x^i) &= \theta\left(\sum_{k=0}^{d+t} (\sum_{i+j=k} a_i \sigma^i(b_j))x^k\right)\\ &= \sum_{k=0}^{d+t} x^{-k}\left(\sum_{i+j=k} a_i\sigma^i(b_j))\right)\\ &= \sum_{k=0}^{d+t}\sum_{i+j=k} x^{-j}x^{-i}\sigma^i(b_j)a_i\\ &= \sum_{k=0}^{d+t}\sum_{i+j=k} x^{-j}b_j x^{-i}a_i\\ &= \theta(\sum_{i=0}^{t} b_i x^i)\theta(\sum_{i=0}^{d} a_i x^i).\end{aligned}$$

It follows that θ is an anti-isomorphism of rings. □

Based on the above proposition, it is now possible to extend the computation of the generator polynomial from the commutative to the non-commutative case. Recall that we may assume the generator polynomial $g(x)$ to be monic, without loss of generality.

Proposition 3. *Consider a code with generator $g(x)$ and parity check polynomial $h(x) = \sum_{i=0}^{k-1} h_i x^i + x^k$, that is $g(x), h(x)$ satisfy $h(x)g(x) = x^n - u$. Suppose that $u^2 = 1$. The Euclidean dual $g^\perp(x)/(x^n-u)$ of the σ-constacyclic code $(g(x))/(x^n-u)$ is a σ-constacyclic code whose generator polynomial is given by*

$$g^\perp(x) = 1 + \sum_{i=1}^{k} \sigma^i(h_{k-i})x^i,$$

or equivalently by the monic polynomial $-ug^\perp(x)$.

Proof. To show that $g^\perp(x)/(x^n - u)$ is a σ-constacyclic code, we need to show that $g^\perp(x)$ is a right divisor of $x^n - u$. We know that $g(x)$ is, namely there exists a polynomial $h(x)$ such that

$$g(x)h(x) = h(x)g(x) = x^n - u.$$

Then, using the anti-isomorphism $\theta : (\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[x;\sigma] \to A$, $\sum_{i=0}^{d} a_i x^i \mapsto \sum_{i=0}^{d} x^{-i}a_i$ of the previous proposition:

$$\begin{aligned} x^k\theta(h(x))\theta(g(x))x^{n-k} &= x^k\theta(g(x)h(x))x^{n-k}\\ &= x^k\theta(x^n-u)x^{n-k}\\ &= x^k(x^{-n}-u)x^{n-k}\\ &= 1 - ux^n = -u(x^n - \frac{1}{u}) = -u(x^n-u),\end{aligned}$$

since $u^2 = 1$. Therefore $x^k\theta(h(x))$ is a left divisor of $x^n - u$, and

$$x^k\theta(h(x)) = x^k\theta(\sum_{i=0}^{k-1} h_i x^i + x^k) = x^k(\sum_{i=0}^{k-1} x^{-i}h_i + x^{-k}) = \sum_{i=0}^{k-1}\sigma^i(h_i)x^{k-i} + 1.$$

By the first part of Proposition 1, $x^k\theta(h(x))$ is also a right divisor of x^n-u. Now that we have shown that $g^{\perp}(x)$ is indeed a σ-constacyclic code, we are left to show that it is the dual of $\mathcal{C}$.

Let $a(x)=\sum_{i=0}^{n-1}a_ix^i$ be the polynomial corresponding to the codeword $a=(a_0,a_1,\dots,a_{n-1})$. Then we denote, for any $0\le l\le n-k-1$, by $d_l(x)$ the polynomial $x^lg^{\perp}(x)$, which corresponds to the codeword :

$$d_l=(0_{1\times l},\sigma^l(h_k),\sigma^{l+1}(h_{k-1}),\dots,\sigma^{l+k}(h_0),0_{1\times(n-k-l+1)}),\ l=0,\dots,n-k-1.$$

Hence, a is orthogonal to the $n-k$ vectors d_l $(0\le l\le n-k-1)$: indeed, note that

$$d_la^T=\sum_{i=l}^{l+k}a_i\sigma^i(h_{l+k-i})$$

which turns out to be the coefficient of x^{k+l} in $a(x)h(x)$, $l=0,\dots,n-k-1$. Since $\deg h(x)=k$, $\deg(a(x)h(x))<n+k$, say $a(x)h(x)=p(x)=\sum_{i=0}^{n+k-1}p_ix^i$, which means that modulo x^n-u,

$$a(x)h(x)=\sum_{i=0}^{n-1}p_ix^i+\sum_{i=n}^{n+k-1}p_ix^i=\sum_{i=0}^{n-1}p_ix^i+\sum_{j=0}^{k-1}p_{j+n}x^j(-u).$$

Moreover, since $a\in\mathcal{C}$, by Proposition 1, we have $a(x)h(x)=0$ modulo x^n-u, implying that the coefficients of x^{k+l}, $l=0,\dots,n-k-1$, are equal to zero. This proves the orthogonality of d_l with respect to a.

Therefore, the $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$-module generated by the codewords d_l $(0\le l\le n-k-1)$ is contained in $\mathcal{C}^{\perp}$.

We now show that the module $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K[d_0,...,d_{n-k-1}]$ has rank $n-k$. Indeed, let $\lambda_0,...,\lambda_{n-k-1}\in\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$ such that $\sum\limits_{l=0}^{n-k-1}\lambda_ld_l=0$. The first coordinate of $\sum\limits_{l=0}^{n-k-1}\lambda_ld_l$ is $\lambda_0h_k=\lambda_0$, so $\lambda_0=0$. Then $\sum\limits_{l=1}^{n-k-1}\lambda_ld_l=0$ and by the same argument, we prove successively that $\lambda_1=0$, ..., $\lambda_{n-k-1}=0$. This proves that the $n-k$ vectors $d_0,...,d_{n-k-1}$ are linearly independent over $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$. □

We remark that in our context of cyclic division F-algebras, u is restricted to F, therefore the polynomial $x^n-u\in(\mathcal{O}_K/p\mathcal{O}_K)[x;\sigma]$ actually has a constant term u which belongs to $\mathcal{O}_F/\mathfrak{p}\mathcal{O}_F$. Therefore the condition $u^2=1$ means that u is of order 2 in a finite field, that is $u=\pm1$. This is however not the case more generally.

Example 4. Let us continue Example 1. We have $x^2+1=(x+\alpha+1)(x+\alpha-1)$ therefore the parity check polynomial is $h(x)=x+\alpha-1$. From Proposition 3, we have that $g^{\perp}(x)=1+\sigma(h_0)x=1+\sigma(\alpha-1)x=1-(\alpha+1)x$. Now left multiple of $g^{\perp}(x)$ modulo x^2+1 are of the form $(b_0+b_1x)(x-(\alpha+1))=[b_0-b_1(\alpha-1)]+[b_0(-\alpha-1)+b_1]x$, so that codewords are

$$(a_0,a_1)=(a_0,(-\alpha-1)a_0).$$

These codewords clearly form the dual code of $\mathcal{C}$, since $\langle(a_0,(-\alpha-1)a_0),y\rangle=0$ for all $y\in\mathcal{C}$.

Example 5. For Example 2, we have $((1,1)+(2,2)x)((1,1)-(2,2)x)=(1,1)+(1,1)x^2$ or equivalently $((3,3)+(1,1)x)((2,2)-(4,4)x)=(1,1)+(1,1)x^2$ with parity check polynomial $h(x)=(2,2)+(1,1)x$. From Proposition 3, we have that

$g^{\perp}(x) = 1+\sigma(h_0)x = 1+\sigma((2,2))x = 1+(2,2)x$. Now left multiple of $g^{\perp}(x)$ modulo x^2+1 are of the form $(b_0+b_1x)(1+(2,2)x) = [b_0 - b_1(2,2)] + [b_0(2,2)+b_1]x$, so that codewords are

$$(a_0, a_1) = (a_0, (2,2)a_0),\ a_0 \in \mathbb{F}_5 \times \mathbb{F}_5,$$

which form the dual code of $\mathcal{C}$, since $\langle (a_0,(2,2)a_0), y\rangle = 0$ for all $y \in \mathcal{C}$. This also shows that $\mathcal{C}$ is self-dual.

Finally we provide another example of self-dual code.

Example 6. Let $K = \mathbb{Q}(\sqrt{2})$ and $F = \mathbb{Q}$. Then $\mathcal{O}_F = \mathbb{Z}$ and $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$. Let $\mathfrak{Q}$ be the quaternion division algebra defined by

$$\mathfrak{Q} = \mathbb{Q}(\sqrt{2}) \oplus \mathbb{Q}(\sqrt{2})e,$$

with $e^2 = -5$. Since $N_{K/F}(a+\sqrt{2}b) = a^2+2b^2$, $a, b \in \mathbb{Z}$, -5 cannot be a norm and $\mathfrak{Q}$ is indeed a quaternion division algebra. We set $\Lambda = \mathbb{Z}[\sqrt{2}] \oplus \mathbb{Z}[\sqrt{2}]e$.

Set $p = 3$, which remains inert in $\mathbb{Q}(\sqrt{2})$. Hence, $\mathbb{Z}[\sqrt{2}]/3\mathbb{Z}[i] \simeq \mathbb{F}_9$ and $\Lambda/3\Lambda \simeq \mathbb{F}_9 \oplus \mathbb{F}_9 e$. Take $\mathcal{I} = (\sqrt{2}+e)\Lambda$. Then $\mathcal{I}$ contains 3 since the norm of $\sqrt{2}+e$ is $N(\sqrt{2}+e) = (\sqrt{2}+e)(-\sqrt{2}-e) = 3$. Let α denote a primitive root of $\mathbb{F}_9$ over $\mathbb{F}_3$, satisfying $\alpha^2+1 = 0$ and as before, $\sigma(\alpha) = \alpha^3$. We have

$$\psi((\sqrt{2}+e)\mathrm{mod}3) = \alpha + x,$$

which is a right divisor of $x^2+5 = x^2+2$ in $\mathbb{F}_9[x;\sigma]$:

$$(x+\alpha)(x+\alpha) = x^2 + \sigma(\alpha)x + (\alpha)x + \alpha^2 = x^2+2.$$

Therefore, the left ideal $(x+\alpha)\mathbb{F}_9[x;\sigma]/(x^2+2)$ is a σ-constacyclic code of length $n = 2$ and dimension 1. Left multiples of $x+\alpha$ modulo x^2+2 are explicitly given by $(b_0+b_1x)(x+\alpha) = [b_0(\alpha)+b_1] + [b_0 + b_1(-\alpha)]x$ and codewords are of the form

$$(a_0, a_1) = (\alpha a_1, a_1),\ a_1 \in \mathbb{F}_9.$$

This code is self-dual, since $u = 2$ satisfies $u^2 = 1$ and $g^{\perp}(x) = 1+\sigma(\alpha)x = 1-\alpha x = -\alpha(\alpha+x)$. Taking the pre-image by ψ, it corresponds to the left-ideal $\mathcal{I}/3\Lambda$, with $\mathcal{I} = (\sqrt{2}+e)\Lambda$.

4.2. **Lattices from Dual Codes.** Recall the proposed variation of Construction A. Given the map

$$\rho : \Lambda \to \psi(\Lambda/\mathfrak{p}\Lambda) = \mathbb{F}_q[x;\sigma]/(x^n - u),$$

compositum of the canonical projection $\Lambda \to \Lambda/\mathfrak{p}\Lambda$ with ψ, we obtained a lattice L given by

$$L = \rho^{-1}(\mathcal{C}) = \mathcal{I}.$$

Now let $\mathcal{C}^{\perp}$ be the dual of $\mathcal{C}$. Then

$$L' = \rho^{-1}(\mathcal{C}^{\perp})$$

is also a lattice.

Example 7. Let us continue Examples 1 and 4. To the code $\mathcal{C}$ given by the left multiples of $(x+1+\alpha) \mod x^2+1$ corresponds the lattice $\rho^{-1}(\mathcal{C}) = (1+i+e)\Lambda$. The dual lattice $\mathcal{C}^{\perp}$ is generated by the left multiples of $1-(\alpha+1)x \mod x^2+1$ to which corresponds the lattice $\rho^{-1}(\mathcal{C}^{\perp}) = (1-(i+1)e)\Lambda$.

We make an obvious observation.

Lemma 4.2. *If $\mathcal{C} \subset \mathcal{C}^{\perp}$, we have the inclusion $L \subset L'$.*

Proof. Let $x \in L$. Then $\rho(x) \in \mathcal{C}$, so $\rho(x) \in C^{\perp}$ and $x \in L'$. □

5. Application to Space-time Codes

We conclude by discussing our motivation to look at the question of defining a variation of Construction A over a cyclic division F-algebra, which comes from space-time coding.

5.1. **Space-Time Coding.** Cyclic division algebras are by now classically used to design space-time codes [13, 14]. Unlike in classical coding theory where codewords are typically vectors with coefficients over finite fields (or finite rings), in the context of space-time coding, codewords are matrices with coefficients coming from number fields, and matrix codewords are obtained as follows. To make the notation easier, we assume for the rest of this section that $u \in \mathcal{O}_F$. To any element $a = a_0 + a_1 e + \cdots + a_{n-1}e^{n-1}$ of Λ, we can associate a matrix in $\mathrm{Mat}_n(\mathcal{O}_K)$ (since $u \in \mathcal{O}_F$) by :

$$M(a) = \begin{bmatrix} a_0 & u\sigma(a_{n-1}) & u\sigma^2(a_{n-2}) & \cdots & u\sigma^{n-1}(a_1) \\ a_1 & \sigma(a_0) & u\sigma^2(a_{n-1}) & \cdots & u\sigma^{n-1}(a_2) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \vdots & \vdots & \vdots & & u\sigma^{n-1}(a_{n-1}) \\ a_{n-1} & \sigma(a_{n-2}) & \sigma^2(a_{n-3}) & \cdots & \sigma^{n-1}(a_0) \end{bmatrix}.$$

The map

$$\begin{aligned} \Lambda &\to \mathrm{Mat}_n(\mathcal{O}_K) \\ a &\mapsto M(a) \end{aligned}$$

is an $\mathcal{O}_K$-algebra injective homomorphism. A space-time code is thus given by $\{M(a),\ a \in \Lambda\}$. The condition that the F-algebra is division is critical, it fulfills one design criterion for space-time codes, namely that $\det(M(a) - M(a')) \neq 0$, $a \neq a'$.

We illustrate this by continuing Example 1.

Example 8. For $q = a + be$ in the natural order $\mathbb{Z}[i] \oplus \mathbb{Z}[i]e$ of the quaternion algebra $\mathfrak{Q}$, $a, b \in \mathbb{Z}[i]$

$$M(q) = \begin{bmatrix} a & -\bar{b} \\ b & \bar{a} \end{bmatrix}$$

where $\bar{\cdot}$ is the non-trivial Galois automorphism of $\mathbb{Q}(i)/\mathbb{Q}$. Let $t = (a+be)(1+i+e)$ be an element of $\mathcal{I} = \Lambda(1+i+e)$ (with $a, b \in \mathbb{Z}[i]$). Then

$$t = a(1+i) - b + (a + b(1-i))e.$$

Hence,

$$M(t) = \begin{bmatrix} a(1+i) - b & -(\overline{a} + \overline{b}(1+i)) \\ a + b(1-i) & \overline{a}(1-i) - \overline{b} \end{bmatrix},$$

and we obtain the space-time code

$$\left\{ \begin{bmatrix} a(1+i) - b & -(\overline{a} + \overline{b}(1+i)) \\ a + b(1-i) & \overline{a}(1-i) - \overline{b} \end{bmatrix},\ a, b \in \mathbb{Z}[i] \right\}.$$

Note that $\mathcal{I} = \rho^{-1}(C)$ is a real lattice with rank 4.

5.2. **Coset Coding.** Let now $v = (v_1, \dots, v_n)$ be an information vector containing the data to be transmitted, which should be mapped to a lattice point in L, where L is used as a lattice code. Mapping a vector with coefficients in a finite ring to a lattice point is not an easy task, and can be facilitated by the use of Construction A. The lattice $L = \rho^{-1}(\mathcal{C}) = \mathcal{I}\Lambda$ may by construction be written as a union of cosets of $\mathfrak{p}\Lambda$, where each coset representative may be chosen to be a codeword in the code $\mathcal{C}$. Namely, if $g(x)$ is a right divisor of $x^n - u$ and if a σ-constacyclic code $\mathcal{C} = (g(x))/(x^n - u) \subset (\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[x;\sigma]/(x^n - u)$ has dimension $k = n - \deg(g)$, since

$$\Lambda/\mathfrak{p}\Lambda \cong (\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[x;\sigma]/(x^n - u)$$

there is an isomorphism

$$\mathcal{I}/\mathfrak{p}\Lambda \cong \mathcal{C}.$$

This allows us to associate in a unique way a coset of $\mathfrak{p}\Lambda$ to a codeword. The mapping from v to a point in L may be done by attributing some information coefficients $v_1, \dots, v_k$ to be encoded using the code $\mathcal{C}$, and the rest of the information coefficients to be mapped to a point in the lattice $\mathfrak{p}\Lambda$. This simplifies the encoding in the cases where $\mathfrak{p}\Lambda$ is a lattice "easier" to label than L, which happens in the original Construction A where this lattice turns out to be a scaled version of $\mathbb{Z}^n$, but also in many cases where $\mathfrak{p}$ gives rise to a lattice isomorphic to $\mathbb{Z}^n$ (or another lattice whose points are easy to label).

Irrespectively of the lattice obtained from $\mathfrak{p}\Lambda$, coset encoding is necessary in the context of wiretap codes. In a wiretap context, a code should not only provide reliability between a transmitter and a receiver, but also ensure confidentiality, should an eavesdropper try to intercept the message. To protect from wiretapping, information symbols are mapped to a codeword in $\mathcal{C}$, while random symbols are picked uniformly at random in the lattice $\mathfrak{p}\Lambda$ to create confusion at the eavesdropper. Wiretap space-time codes have been studied in [15], where coset encoding of space-time codes is assumed. However, no concrete way to do so was proposed. The construction of the lattice $L = \rho^{-1}(\mathcal{C}) = \mathcal{I}$ as presented in this work thus enables coset encoding for wiretap space-time codes.

6. Future Work

In this paper, we presented a construction of lattices from constacyclic codes over skew-polynomials, which can be interpreted as a variation of the well known Construction A of lattices from linear codes. The starting point was the quotient $\Lambda/\mathfrak{p}\Lambda$ of a given order Λ from a cyclic division F-algebra, which is motivated by applications of such algebras to space-time coding. Natural future research directions include:

- To continue the study of constacyclic codes over $(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[x;\sigma]/(x^n - u)$, in particular by replacing the polynomial $x^n - u$ with a more general polynomial $f(x)$. This may include looking at the characterization of self-dual codes. One could alternatively consider duality with respect to a Hermitian inner product.
- Linking the properties of the constacyclic code $\mathcal{C}$ to that of the lattice $L = \rho^{-1}(\mathcal{C})$: there are standard duality results for the classical Construction A, relating the dual lattice of L^* with L', or the weight enumerator of the code with the theta series of the lattice, which have not yet been considered.

This leads to further properties of lattices that could be explored, such as extremality and modularity.

- Design of wiretap space-time codes: this consists of choosing the cyclic division F-algebra A, the corresponding two-sided ideal $\mathcal{I}$ and constacyclic code $\mathcal{C}$, to optimize the confusion at the eavesdropper.

References

[1] J.H. Conway and N.J.A Sloane, "Sphere Packings, Lattices and Groups", Springer.

[2] G. D. Forney, Coset Codes Part I: Introduction and geometrical classification, *IEEE Trans. on Inform. Theory*, vol 34, no 5, 1988.

[3] W. Ebeling, Lattices and Codes, A Course Partially Based on Lectures by Friedrich Hirzebruch, Springer, in the series Advanced Lectures in Mathematics.

[4] C. Bachoc, Applications of Coding Theory to the Construction of Modular Lattices, *Journal of Combinatorial Theory*, 1997.

[5] A. Bonnecaze, P. Sole, A.R. Calderbank, Quaternary Qudratic Residue codes and Unimodular Lattices, *IEEE Trans. on Information Theory*, vol. 41, no 2, March 1995.

[6] D. Boucher and F. Ulmer, "Coding with skew polynomial rings", *Journal of Symbolic Computation*, vol. 44, 2009.

[7] D. Boucher, W. Geiselmann and F. Ulmer, Skew Cyclic Codes, *Applied Algebra in Engineering, Communication and Computing*, 18 (2007), 379 - 389

[8] D. Boucher, F. Ulmer, P. Solé, "Skew Constacyclic Codes over Galois Rings" *Advances in Mathematics of Communications*, 2, 273-292 (2008).

[9] F. Oggier and B. A. Sethuraman, "Quotients of Orders in Cyclic Algebras and Space-Time Codes", *Advances in Mathematics of Communication*, vol. 7, November 2013, 441-461.

[10] J. Ducoat, F. Oggier, "Lattice Encoding of Cyclic Codes from Skew-polynomial Rings", proceedings of the Fourth International Castle Meeting on Coding Theory and Applications, Palmela, 2014.

[11] F. Oggier and J.-C. Belfiore, "Enabling Multiplication in Lattice Codes via Construction A", proceedings of the IEEE International Workshop on Information Theory, Sevilla, 2013.

[12] M. Artin,"Noncommutative Rings", 1999.

[13] B. A. Sethuraman and B. S. Rajan and V. Shashidhar, "Full-diversity, high-rate space-time block codes from division algebras", *IEEE Trans. on Inform. Theory*, vol. 49, no 10, 2003.

[14] G. Berhuy and F. Oggier, "An Introduction to Central Simple Algebras and Their Applications to Wireless Communication", AMS, 2013.

[15] J.-C. Belfiore and F. Oggier, "An Error Probability Approach to MIMO Wiretap Channels", *IEEE Transactions on Communications*, vol. 61, no. 8, 2013.

Division of Mathematical Sciences, School of Physical and Mathematical Sciences,
Nanyang Technological University, Singapore.
E-mail address: jerome.ducoat@gmail.com
E-mail address: frederique@ntu.edu.sg